JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 1, pp. 71-77, January 2020
https://doi.org/10.9708/jksci.2020.25.01.071

Proposed image encryption method using PingPong256

Ki-Hwan Kim*, Hoon Jae Lee**, Young Sil Lee**

*Graduate Student, Dept. of Ubiquitous IT, Dongseo University, Busan, Korea
**Professor, Div. of Information and Communication Engineering, Dongseo University, Busan, Korea
**Professor, Div. of Information and Communication Engineering, Dongseo University, Busan, Korea

[Abstract]

In this paper, we propose a method in which PingPong256 combines LFSR and variable clock to generate an irregular PRNG and use it for image encryption. PingPong256 is guaranteed an extended period based on the two LFSRs, and the variable clock is a structure that outputs the result of operating a predetermined clock in one operation by referring to the state of the different LFSR. A variable clock is characterized by the difficulty of predicting the output at any time because the choice increases with time. PingPong256 combines the advantages of LFSR and variable clock, the convenience of hardware and software implementation, and the benefits of sensitivity and irregular periods. Also, the statistical safety was verified using the NIST SP800-22, the safety of the proposed method, and the sensitivity of the image change was tested using NPCR and UACI.

▸ **Key words**: Image Encryption, PingPong256, NIST SP800-22, NPCR, UACI

[요 약]

본 논문에서 우리는 PingPong256은 LFSR과 가변클록을 결합하여 불규칙한 PRNG를 생성하고 이를 이미지 암호화에 활용하는 방법을 제안한다. PingPong256은 2개의 LFSR을 기반으로 긴 주기가 보장되며, 가변클록은 서로 다른 LFSR의 상태를 참조하여 1회 동작시 임의의 클록만큼 동작한 결과를 출력하는 구조이다. 가변클록은 시간이 경과함에 따라 선택지가 증가하기 때문에 임의의 시간에 출력을 예측하기 어렵다는 특성으로 나타난다. PingPong256은 LFSR과 가변클록과 하드웨어 및 소프트웨어 구현의 편리함이라는 장점 및 민감성과 불규칙한 주기라는 장점을 결합한 것이다. 또한 NIST SP800-22를 사용하여 통계적 안전성을 검증하고 제안 된 방법의 안전성을 확인하고 NPCR 및 UACI를 사용하여 이미지 변화의 감도를 테스트 하였습니다.

▸ **주제어**: 이미지 암호화, PingPong256, NIST SP800-22, NPCR, UACI

• First Author: Ki-Hwan Kim, Corresponding Author: Young Sil Lee
*Ki-Hwan Kim (ghksdl90@naver.com), Dept. of Ubiquitous IT, Dongseo University
*Hoon Jae Lee (hjlee@dongseo.ac.kr), Div. of Information and Communication Engineering, Dongseo University
*Young Sil Lee (youngsil.lee0113@gmail.com), Div. of Information and Communication Engineering, Dongseo University
• Received: 2019. 12. 24, Revised: 2020. 01. 06, Accepted: 2020. 01. 06.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

시간이 경과함에 따라서 이미지 센서는 고화질 및 고해상도 사진을 표현할 수 있도록 연구되고 있다. 이미지 데이터는 많은 양의 정보를 함축할 수 있으며, 정보의 가치에 따라서 암호화가 필요할 수 있다. 이와 유사한 연구로 [1]에서는 지문 이미지를 암호화하고 위조를 방지하거나 [2]와 같이 우주환경에서 암호화된 이미지 데이터가 잡음에 대한 영향을 받는지 확인하는 등 이미지에 대한 다양한 연구가 진행되고 있다. 또 다른 방법으로 IoT환경에서 사람을 식별하는 방법으로 카메라와 AI를 활용하여 이미지 암호화는 2가지 범주로 구분할 수 있다. 먼저, 이미지 정보를 암호화 하는 방법으로 Advanced Encryption Standard(AES)를 활용하여 이미지 데이터를 암호화하는 방법이다[3,4]. 이미지를 암호화 하는 방법은 병렬연산을 활용하여 암호화와 복호화를 효율적으로 수행할 수 있다는 장점이 있지만 실시간 데이터를 처리하기에 적합하지 못하다. 다른 방법은 의사난수 생성기에 해당하는 Pseudorandom Number Generator(PRNG)를 생성하여 이미지와 결합하여 암호화하는 방식이다. PRNG는 완벽에 가까운 난수를 생성할 수 있는 생성기를 말하며, PRNG를 생성하는 방법은 AES Output-FeedBack(OFB)모드, Hash 함수, Chaotic map 등이 존재한다[4-9]. PRNG를 활용하는 방식은 PRNG에 높은 의존성을 가지고 있어서 PRNG의 안전성을 증명하는 것이 필요하지만 암호화 방식보다 빠른 처리가 가능하여 연속적인 처리에 적합하다.

PRNG를 생성하는 추가적인 방법으로 PingPong256이 있다. PingPong256은 길이가 다른 2개의 LFSR을 사용하여 긴 주기를 보장하며, 매번 출력마다 임의의 클록만큼 추가적으로 동작하여 시간에 누적됨에 따라 경우의 수가 증가하는 구조를 가지고 있다.

본 논문에서는 PRNG로 PingPong을 사용하여 이미지 암호화에 활용하는 것을 실험을 통해 확인한다. 2장에서는 PingPong 알고리즘의 구조와 안전성을 살펴보고 3장에서는 PingPong을 통해 PRNG를 생성하여 이미지와 결합한 결과를 살펴보고, 4장에서 논문의 결론을 내리면서 추가연구 방향을 살펴본다.

II. Proposed structure

1. PingPong 256 structure and Safety

PingPong256(PP256)은 그림 1과 같이 서로 다른 길이의 Linear Feedback Shift-Register(LFSR)를 사용하며, 가변클록(f_a, f_b)과 메모리(c_i, d_i)를 가지고 있어 모든 주기를 저장할 수 없는 특징을 가지고 있어서 역방향 분석이 거의 불가능하다[10].

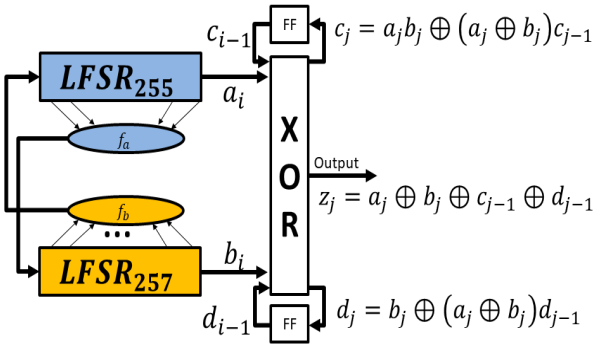

Fig. 1. PingPong256 Structure.

PingPong256의 주기(P)는 식(1) 그리고 선형복잡도(LC)는 식(2)와 같다.

$$P \geq 2^{4.6} \times 2^{\lceil (512-11)/2 \rceil} \approx 2^{256} \quad (1)$$

$$LC \geq 2^{4.6} \times 2^{\lceil (512-11)/2 \rceil} \approx 2^{256} \quad (2)$$

PingPong 256의 안전성을 검사하는 방법으로 통계적 검증이 존재한다. 통계적 검증의 경우 NIST에서는 PRNG의 객관적인 안전성을 검증하는 방법으로 NISR SP800-22가 있고 이때 권장하는 입력 데이터의 길이는 10^6비트이다[11]. PingPong256의 초기값을 표 1과 같이 설정하여 10^6비트 데이터를 생성하였다.

Table 1. PingPong256 Initialization value.

Type	Date
$LFSR_{255}$	75165D49, 27D39935, DD3BC370, A6D51456, 1D459752, 49B4E64D, 774EF0DC, 14DAA29A
$LFSR_{257}$	D5135512, 5B951D95, 3665265B, 4F744D54, B544D544, 96E54765, 4D994916, D3DD137E, 1

NIST SP800-22는 생성한 데이터가 난수성이라면 모든 테스트에서 p-value가 0.01을 넘어야한다고 명시되어 있다. 실험결과 표 2를 통해 모든 실험에서 p-value가 0.01을 넘는 것을 확인할 수 있다.

Table 2. NIST SP800-22 result

	Type of Test		p-Value (>0.01)	Result
1	Frequency(Monobit)		0.3411	Random
2	Frequency Test within a Block		0.7218	Random
3	Run		0.0947	Random
4	Longest Run of Ones in a Block		0.8769	Random
5	Binary Matrix Rank		0.0217	Random
6	Discrete Fourier Transform (Spectral)		0.9707	Random
7	Non-Overlapping Template Matching		0.4351	Random
8	Overlapping Template Matching		0.7811	Random
9	Maurer's Universal Statistical		0.3566	Random
10	Linear Complexity		0.0652	Random
11	Serial		0.7764	Random
			0.8760	Random
12	Approximate Entropy		0.3385	Random
13	Cummulative Sums (Forward)		0.3413	Random
14	Cummulative Sums (Reverse)		0.5441	Random
15	Random Excursions	4	0.5034	Random
		3	0.4017	Random
		2	0.0607	Random
		1	0.6690	Random
		-1	0.8181	Random
		-2	0.6566	Random
		-3	0.2014	Random
		-4	0.1176	Random
16	Random Excursions Variant	-9	0.3630	Random
		-8	0.2642	Random
		-7	0.1765	Random
		-6	0.2290	Random
		-5	0.3474	Random
		-4	0.3910	Random
		-3	0.3204	Random
		-2	0.3074	Random
		-1	0.4735	Random
		+1	0.2323	Random
		+2	0.1292	Random
		+3	0.2951	Random
		+4	0.6131	Random
		+5	0.6730	Random
		+6	0.70263	Random
		+7	0.69584	Random
		+8	0.4443	Random
		+9	0.2215	Random

2. Image Encryption Decryption Method

초기화는 PingPong256의 모든 메모리를 0으로 설정하고 두 개의 LFSR의 총 512비트를 설정하며, 1000회 동작 후 이미지 암호화에 사용하였다. 이미지의 암호화는 스트림 방식으로 식 (3)과 같이 이미지, PingPong256 그리고 이전 픽셀의 암호화 결과를 사용했다. P_i는 원본 이미지의 i번째 픽셀, R_i는 PingPong256을 사용하여 생성한 난수 이미지의 I번째 픽셀 그리고 C_i는 암호화된 이미지의 I번째 픽셀을 의미한다. 이미지 암호화는 원본 이미지와 PingPong256 그리고 이전에 암호화된 이미지 픽셀 정보를 모두 포함하게 된다. 그림 2는 식 (3)의 동작을 픽셀별로 연산 순서를 나타낸 것이다.

$$C_i = P_i \oplus R_i \oplus C_{i-1} \tag{3}$$

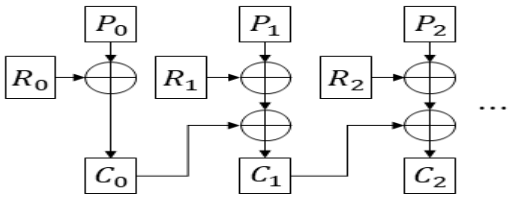

Fig. 2. Encrypt image using PingPong256.

복호화의 경우 PingPong256의 초기값을 동일하게 설정할 경우 식 (4)와 같이 올바른 이미지로 해독하는 것이 가능하다. 그림 3은 식(4)의 동작을 픽셀별로 연산 순서를 나타낸 것이다.

$$P_i = C_i \oplus R_i \oplus C_{i-1} \tag{4}$$

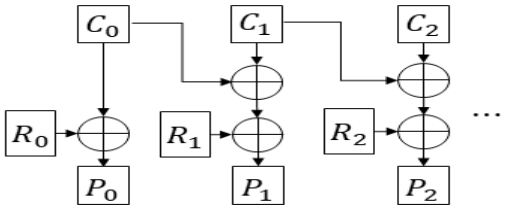

Fig. 3. Decrypt image using PingPong256.

그림 4와 같이 (a)의 512*512의 크기인 Lena이미지와 (b)의 PP256 난수 이미지를 결합한 (c)의 암호화 이미지를 (d)와 같이 올바른 이미지로 복원할 수 있다.

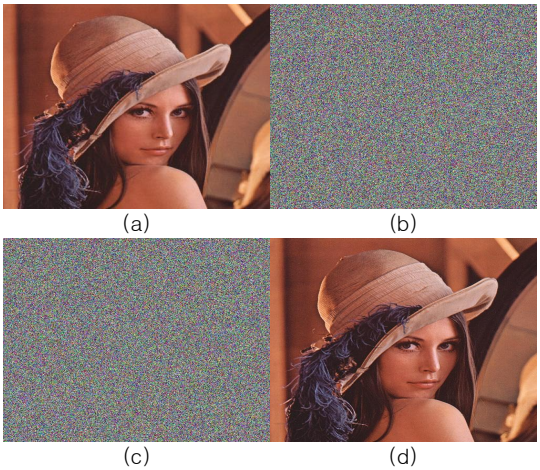

Fig. 4. Using image encryption of PingPong256 (a)Plain Image of Lena, (b)Random image of PP256, (c)Encryption image of Lena, (d)Decrypt image of Lena.

III. Key space

제안하는 이미지 암호화는 PingPong256에 높은 의존도를 보이고 있다. 따라서 PingPong256의 키 공간과 키 민감도의 안전성이 중요하다. 따라서 PingPong256의 키 공간을 분석하고 이미지 암호화에 따른 결과 예측을 살펴본다.

3.1 Key space analysis

올바른 암호화 체계에는 무차별 대입 공격을 방어 할 수 있는 충분한 비밀키 공간이 필요하다. PingPong256은 총 512비트의 초기값이 존재하며, 모든 경우의 수는 2^{512}에 해당한다. 제안된 암호화 알고리즘의 초기키 공간은 무차별 대입 공격에 견딜 수 있을 만큼 충분히 크다.

또한 가변 클록의 경우 1에서 4까지의 무작위 클록이 선택되기 때문에 초기값을 모르는 경우 각 LFSR당 1/4확률로 선택을 강요받으며, 모든 LFSR로 확대할 경우 1/16 확률로 선택해야한다. 시간이 경과하면서 모든 경우의 수가 급격하게 늘어나 결국 가변 클록으로 초기값이 더 혼돈되어 비밀키 예측이 불가능하게 된다.

3.2 Key sensitivity analysis

올바른 암호화 체계는 비밀키에 매우 민감해야한다. 비밀키 감도는 1 비트의 변화에도 동일한 일반 이미지의 암호화 된 이미지가 완전히 달라야 함을 의미한다. 또한 초기값에 약간의 차이가 있으면 해독 된 이미지가 원본 이미지와 크게 달라야 한다. 그림 5는 실험결과로 (a)는 Table 1의 값을 기준으로 생성한 흑백 이미지이며, (b)는 (a)의 초기값에 LFSR255에서 마지막 비트 반전하였다. (c)는 (a)의 초기값에서 LFSR257에서 마지막 비트를 반전한 결과이다. 하지만 육안으로는 뚜렷한 차이를 느낄 수 없기 때문에 and 연산을 통해 각각의 이미지에서 동일한 값을 추출해 보았다. (d),(e),(f)는 각각 (a)and(b), (a)and(c), (b)and(c)의 연산결과이며, 1비트의 변화가 전체적으로 변화를 유발한다고 볼 수 있다.

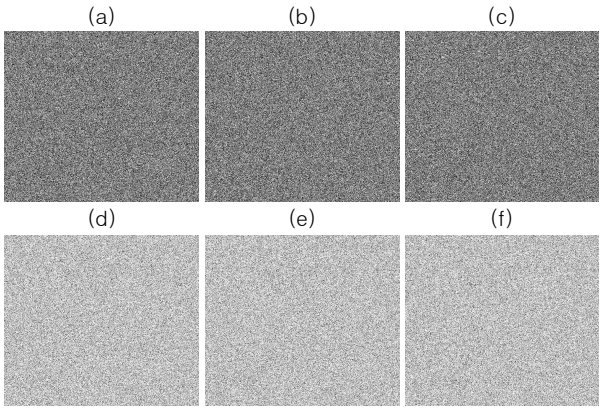

Fig. 5. Compare PingPong256 Image. (a)Reference to Table 1 value, (b) LFSR255+1, (c) LFSR257-1, (d) (a)and(b), (e) (a)and(c), (f) (b)and(c).

IV. The Proposed Scheme

4.1 Histogram analysis

히스토그램은 이미지의 픽셀 값 분포를 보여준다. 좋은 암호화 방법을 사용한 이미지는 통계적 공격에 저항하기 위해 균일한 히스토그램을 가져야한다[12]. 일반적으로 흑백 이미지의 경우 컬러 이미지보다 특징을 추출하기에 용이하여 히스토그램 분석에는 흑백이미지를 기본적으로 사용하고 있다. 일반 이미지의 히스토그램 및 해당 암호 이미지가 그림 6과 같다. 분석 결과 암호화 된 이미지가 일반 이미지보다 다소 균일함을 분명히 나타낸다.

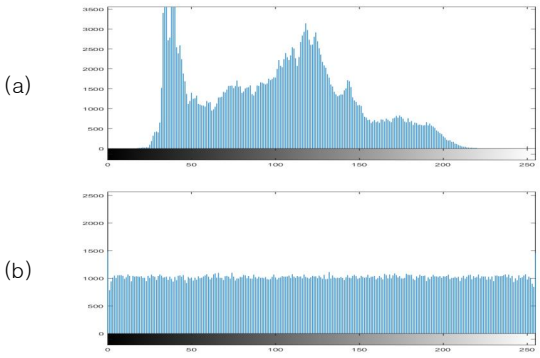

Fig. 6. Histogram of Lena. (a)Plain image, (b) Cipher image.

4.2 Image Entropy Analysis

엔트로피는 이미지의 평균 정보량을 반영한다. s가 정보의 원천을 나타내면, 엔트로피는 식 (5)처럼 같이 정의된다[00].

$$H(s) = -\sum_{i=0}^{2^n-1} p(s_i) \times \log_2(p(s_i)) \quad (5)$$

여기서 $p(s_i)$는 정보 s_i의 확률을 나타내고 2^n은 정보의 총 상태 수를 나타낸다. 실험에서 s_i는 그레이 스케일 값이고 2^n은 256으로 설정되어 있다.

정보 엔트로피가 클수록 픽셀 값 분포가 균일하고 이미지 보안 성능이 향상된다. 이론적으로, 암호화된 이미지의 경우 최대 엔트로피 값은 최대 8이 될 수 있다 [13-15]. 표 2는 원본 이미지와 암호화 방식이 다른 암호화 된 이미지의 정보 엔트로피를 보여줍니다. 암호화 된 이미지의 엔트로피는 특히 제안 된 체계에서 8에 더 가깝다는 것을 알 수 있습니다. 결과는 알고리즘이 다소 안전하다는 것을 보여줍니다.

Table 3. The information entropy for original and cipher image schemes.

Image	Original	Liu's scheme[13]	Propose Cipher
Entropy	7.270652	7.99730	7.998052

4.3 Correlation analysis

일반적으로 원본 이미지는 가로, 세로 및 대각선 방향을 포함하여 인접한 픽셀과 큰 상관관계가 있다. 좋은 암호화 체계는 인접한 픽셀의 상관관계를 효과적으로 줄여야한다. 상관관계 분석은 상관 계수를 사용하여 인접 픽셀 간의 상관관계를 분석하고 제안 된 방식을 추가로 확인한다. 상관계수는 식 (6)과 같이 계산될 수 있다.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (6)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (7)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \quad (8)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \quad (9)$$

식 (6)은 피어슨 상관계수 공식으로 두 변수간의 관련성을 구하기 위해 보편적으로 이용되고 있다. 피어슨 상관계수의 범위는 +1~-1이며, 해석하는 방법은 r_{xy}을 기준으로 1에 가까울수록 강한 상관관계, -1에 가까울수록 음의 상관관계, 0에 가까울수록 무시될 수준의 상관관계를 의미한다. 식(7)~식(9)는 식(6)에 대한 세부 함수에 해당한다. 표 4는 원본 이미지와 암호화된 이미지의 상관분석 결과이다.

Table 4. Compellation analysis.

	Original image			Encryption image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.951897	0.951897	0.972564	0.019790	-0.023263	-0.023263

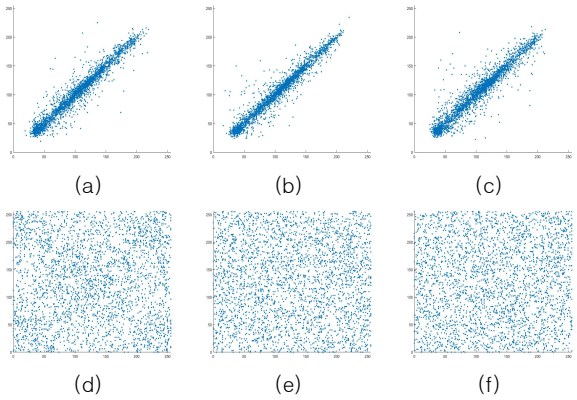

Fig. 7. Distribution of adjacent pixel sequence pairs of Lena image. (a)horizontal of plain image, (b) vertical of plain image, (c) diagonal of plain image, (d) horizontal of encrypted image, (e) vertical of encrypted image, (f) diagonal of encrypted image.

표 4를 통해 원본 Lena 이미지는 수평, 수직, 대각으로 인접하는 픽셀 모두 강한 양의 상관관계가 있고 암호화한 Lena 이미지는 수평, 수직, 대각으로 인접하는 픽셀 모두 0에 인접하여 무시될 수준의 상관관계의 특성을 나타내고 있다. 그림 7은 표 4의 결과를 표현한 것으로 (a~c)는 각각 원본 Lena 이미지의 수평, 수직, 대각으로 인접한 픽셀 그리고 (d~f)는 원본 Lena 이미지를 암호화하여 인접한 픽셀 시퀀스 쌍의 수평, 수직, 대각 상관관계를 나타낸 것이다.

3.4 Sensitivity analysis

이미지 유형을 활용한 검증으로는 Number of Changing Pixel Rate(NPCR)와 Unified Averaged Changed Intensity (UACI)를 활용하는 방법이 존재한다 [16,17]. 이미지 크기가 M*N일 경우 $D(i,j)$는 서로 다른 사진에서 같은 위치의 픽셀이 서로 다를 경우 1 같은 경우 0을 출력하는 방식이다. $c(i,j)$는 서로 다른 사진에서 같은 위치의 픽셀을 정수로 치환하여 뺀 절대값을 말한다.

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\% \quad (10)$$

$$UACI = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|c_1(i,j) - c_2(i,j)|}{255} \times 100\% \quad (11)$$

표 5, 표 6의 결과를 통해 대부분의 검증기준을 만족하는 것을 볼 수 있다.

Table 5. Test Image Size M-by-N 512-by-512 NPCR Randomness test

Test Image Size M-by-N 512-by-512		level(%)		
		0.05	0.01	0.001
Color	Value(%)	99.5893	99.5810	99.5717
Red	99.6208	PASS	PASS	PASS
Green	99.6059	PASS	PASS	PASS
Blue	99.6002	PASS	PASS	PASS

Table 6. Test Image Size M-by-N 512-by-512 UACI Randomness test

Test Image Size M-by-N 512-by-512		level(%)		
		0.05	0.01	0.001
Color	Value(%)	33.3730 ~ 33.5541	33.3445 ~ 33.5826	33.3115 ~ 33.6156
Red	33.4467	PASS	PASS	PASS
Green	33.4098	PASS	PASS	PASS
Blue	33.5464	PASS	PASS	PASS

V. Conclusions

이미지 암호화는 다양한 방법이 있지만 약간의 노이즈와 왜곡으로는 올바른 데이터 암호화를 할 수 없다. 따라서 이미지 암호화하기 위해서는 반드시 모든 픽셀에 영향을 주어야 한다. PingPong의 구조는 연속된 데이터 생성에 적합하고 통계적으로 안전한 결과를 출력할 수 있다는 것을 NIST SP800-22로 확인하고 비밀키 공간 및 비밀키 민감도 분석을 통해 무차별 공격에 대한 저항성이 충분한 것으로 확인했다. 본 논문에서는 PingPong을 사용하여 이미지 암호화하는 것이 가능하고 암호화된 이미지는 다양한 특징 분석에서 난수적인 특징을 가지고 있다는 결과를 얻을 수 있었다. PingPong은 하드웨어, 소프트웨어적 구현이 용이한 LFSR과 배타적 논리합 그리고 Shift 연산으로 이루어져 있다. 또한 AES와 같이 다수의 라운드 연산을 요구하지 않기 때문에 에너지관리에서 유리할 수 있다. 추후 연구에서는 IoT환경에서 AES와 PingPong 알고리즘의 소비전력과 병렬연산 구조 비교를 통해 연구방향성을 고려하고자 한다.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (grant number: 2018R1C1B5043135) and it was also support by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and technology (grant number: NRF2016R1D1A1B01011908).

REFERENCES

[1] Vaibhav B Joshi and Mehul S Raval, "An Improved Commutative Reversible Watermarking and Encryption for Fingerprint Image." September. 2019. URL:https://osf.io/kvxah/download

[2] KiHwan Kim, HyeongRag Kim, HoonJae Lee, Young-Jae Ryu, “Analysis of Noise Sensitivity due to Image Wireless Transmission,” Journal of the Korea Institute of Information and Communication Engineering(JKIICE), Vol. 22, No. 1, pp. 211-220, January 2018. DOI: https://doi.org/10.6109/jkiice.2018.22.1.211

[3] Amandeep Singh, Praveen Agarwal and Mehar Chand, "Image Encryption and Analysis using Dynamic AES," IEEE. 2019 5th International Conference on Optimization and Applications (ICOA), April 2019. DOI: 10.1109/ICOA.2019.8727711

[4] Yong Zhang, "Test and verification of AES used for image encryption," 3D Research, Vol. 9, No. 3, pp. 1, March 2018. DOI: 10.1007/s13319-017-0154-7

[5] Yuqin Lue, Jin Yu, Wenrui Lai, Lingfeng Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," Multimedia Tools and Applications, pp.1-21, April 2019. DIO: 10.1109/ICCSIT.2010.5564894

[6] Vinod Patidar, N.K. Pareek, G. Purohit, K.K. Sud, “A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption,” ELSEVIER.

[7] Shuqin Zhu, Congxu Zhu and Wenhong Wang, “A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256,” Entropy, Vol.20, No.9, September 2018. DOI: 10.3390/e20090716

[8] Amna Shifa, Muhammad S. Afgan, Mamoona N. Asghar, Martin Fleury, Imran Memon, Saima Abdullah AND Nadia Rasheed, “Joint crypto-stego scheme for enhanced image protection with nearest-centroid clustering,” IEEE Access, Vol. 6, pp.16189-16206, March 2018. DOI: 10.1109/ACCESS.2018.2815037

[9] El-Habib Bensikaddour, Youcef Bentoutou and Nasreddine Taleb, "Satellite image encryption method based on AES-CTR algorithm and GEFFE generator." 2017 8th International Conference on

Recent Advances in Space Technologies (RAST), IEEE, June 2017. DOI: 10.1109/RAST.2017.8002953

[10] Ki-Hwan Kim and HoonJae Lee. "Proposal of multi-channel operation technique using PingPong256." 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), September 2018, DOI: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00222

[11] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray and San Vo, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” National Institute of Standards and Technology, 2001.

[12] Shi Liu, Changliang Guo and John T.Sheridan, "A review of optical image encryption techniques." Optics & Laser Technology, Vol. 57, pp. 327-342, April 2014. DOI: 10.1016/j.optlastec.2013.05.023

[13] Lu Xu, Zhi Li, Jian Li and Wei Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” Opt. Lasers Eng, Vol. 78, pp. 17−25, March 2016. DOI: 10.1016/j.optlaseng.2015.09.007

[14] Xing-Yuan Wang, Ying-Qian Zhang and Xue-Mei Bao, “A novel chaotic image encryption scheme using DNA sequence operations,” Opt. Lasers Eng. Vol. 73, pp. 53−61, October 2015. DOI:10.1016/j.optlaseng.2015.03.022

[15] Ting Hu, Ye Liu, Li-Hua Gong and Chun-Juan Ouyang, “An image encryption scheme combining chaos with cycle operation for DNA sequences,” Nonlinear Dyn, Vol. 87, pp. 51−66, August 2017. DOI: https://doi.org/10.1007/s11071-016-3024-6

[16] Ye Liu, Jun Wang, Jinghui Fan and Lihua Gong, “Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences,” Multimed. Tools Appl, Vol. 75, pp. 4363−4382, February 2015. DOI: https://doi.org/10.1007/s11042-015-2479-7

[17] Yue Wu, Joseph P. Noonan and Sos Agaian, "NPCR and UACI randomness tests for image encryption," Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), Vol. 1, No. 2, pp. 31~38, April 2011. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.2127&rep=rep1&type=pdf

Authors

Ki-Hwan Kim received the B.S., M.S. degree in Computer Networking from Dongseo University, Republic of Korea in 2015. Mr. Kim is now a Ph.D. student in the ubiquitous IT department at Dongseo Graduate School in 2017. His research interests are cryptography, Information security and Side-Channel Attack(SCA).

Hoon Jae Lee received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. Dr. Lee had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc

She received the B.S. degree in Electrical engineering and the M.S. degree in Electrical engineering, both from the Dongseo University, Busan, South Korea in 2006 and 2010 respectively. And her received Ph.D. degree in Ubiquitous IT from Dongseo University, Busan, South Korea in 2015. Dr. Lee works for Department of Computer Engineering of Dongseo University as an associate professor. Her research area covers security including healthcare system, RFID or WSN technologies.